CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA

SANS

Caso de éxito:

Galicia fortalece su resiliencia cibernética regional mediante un programa público de formación SANS

Entrevista con **Carlos Vázquez Mariño**

RESUMEN EJECUTIVO

Este caso de éxito describe cómo el gobierno regional de Galicia, España, ha reforzado su resiliencia cibernética mediante un programa estratégico de formación pública en ciberseguridad. En 2024, cuando España se situó como el quinto país del mundo con mayor número de ataques de ransomware, el Centro de Novas Tecnoloxías de Galicia (CNTG) lanzó una iniciativa para ofrecer formación SANS a la ciudadanía de toda la región, incluyendo tanto a personas empleadas como desempleadas.

El programa comenzó con una evaluación sistemática de necesidades liderada por Amtega, la Agencia para la Modernización Tecnológica de Galicia. En estrecha colaboración con actores del sector público y privado, Amtega identificó las brechas de competencias en ciberseguridad más críticas dentro de la fuerza laboral regional. A través del proceso de contratación pública en España, SANS Institute fue seleccionado como proveedor de formación, basándose en su reputación global y en el valor de sus certificaciones GIAC, reconocidas por la industria.

En 2024, la primera promoción contó con 20 estudiantes que completaron los cursos SEC504 y FOR508, alcanzando índices de satisfacción superiores a 9 sobre 10 y reportando avances profesionales medibles, incluidos incrementos salariales. Las empresas locales también se beneficiaron, ya que los empleados recién certificados permitieron a las organizaciones cumplir los requisitos de licitaciones que exigen profesionales de ciberseguridad certificados.

El éxito inicial del programa ha establecido un modelo sostenible en el que la inversión pública en educación en ciberseguridad genera retornos medibles en toda la economía regional. Ya están en marcha planes para ampliar el currículo e incluir los cursos SEC556 y FOR572.

El enfoque colaborativo de Galicia demuestra cómo los gobiernos regionales pueden abordar simultáneamente la escasez inmediata de competencias en ciberseguridad y construir resiliencia cibernética a largo plazo. Esta iniciativa ofrece un modelo replicable para otras comunidades autónomas y gobiernos de todo el mundo que buscan fortalecer su postura de ciberseguridad mediante formación accesible y de alta calidad.

Carlos Vázquez Mariño

Director, Centro de Novas Tecnoloxías de Galicia (CNTG)

Regional Ministry of Employment, Trade and Emigration, Xunta de Galicia

Carlos Vázquez es licenciado en Informática por la Universidad de Coruña y funcionario de carrera del Cuerpo de Profesores de Enseñanza Secundaria, especialidad Informática. Ha desempeñado el cargo de Subdirector General de Sistemas de Información en la Consellería de Educación (2009–2012); Director del Área de Soluciones Tecnológicas Sectoriales en la Agencia para la Modernización Tecnológica de Galicia (AMTEGA) (2012–2020); Subdirector General de Formación Profesional en la Consellería de Educación (2020–2022); y es Director del CNTG desde 2023.

GALICIA FORTALECE SU RESILIENCIA CIBERNÉTICA REGIONAL MEDIANTE UN PROGRAMA PÚBLICO DE FORMACIÓN SANS.

*"Los profesionales que finalizan la formación de SANS obtienen una **ventaja competitiva** que justifica plenamente la **inversión realizada.**"*

La transformación digital ha llegado a todas las comunidades autónomas de España, pero pocas han abordado el desarrollo del talento en ciberseguridad de forma tan estratégica como Galicia. En 2024, España experimentó un aumento significativo de ciberamenazas, situándose en quinto lugar mundial en ataques de ransomware, con 58 incidentes reportados en el primer semestre del año, un incremento del 23 por ciento respecto a 2023[1].

En este contexto, el gobierno autonómico de Galicia ha lanzado un ambicioso programa público de formación en ciberseguridad que ofrece oportunidades de desarrollo profesional a los ciudadanos de toda la región, estableciendo nuevos estándares sobre cómo los gobiernos pueden fortalecer la resiliencia cibernética regional mediante la inversión pública estratégica en el desarrollo de competencias.

El Centro de Novas Tecnoloxías de Galicia (CNTG) ha sido uno de los organismos del gobierno gallego que ha liderado esta iniciativa. El CNTG es un centro público de formación profesional dependiente de la Consellería de Emprego de la Xunta de Galicia, que atiende tanto a ciudadanos empleados como desempleados que buscan oportunidades en el sector tecnológico. La misión del centro va más allá de la formación en TI tradicional: se trata de construir lo que su director, Carlos Vázquez, describe como un colectivo profesional dinámico y técnicamente preparado que pueda hacer frente a los desafíos de ciberseguridad a los que se enfrenta esta comunidad autónoma del noroeste de España.

Identificación de necesidades regionales

La evolución del CNTG hacia la formación en ciberseguridad no se produjo de forma aislada. La misión más amplia del centro de desarrollar experiencia técnica se cruzó con una creciente necesidad regional identificada por socios gubernamentales. Esta convergencia terminaría reformulando la manera en que Galicia aborda el desarrollo del talento en ciberseguridad.

El catalizador llegó a través de Amtega, "*una unidad independiente dentro de la estructura del gobierno autonómico gallego que gestiona las políticas y acciones de ciberseguridad en Galicia, particularmente en las administraciones públicas*", explica Vázquez. La Agencia para la Modernización Tecnológica de Galicia (Amtega) está adscrita a la Consellería de Facenda e Administración Pública de la Xunta de Galicia, con objetivos principales que incluyen definir, desarrollar e implementar estrategias, políticas y gestión de ciberseguridad para el sector público autonómico.

El enfoque de Amtega para identificar necesidades de formación en ciberseguridad se basa en el contacto directo con la comunidad profesional de la región. "*A través de conversaciones continuas con actores de la ciberseguridad de los sectores público y privado, Amtega identificó carencias específicas de competencias que afectaban a la resiliencia cibernética regional*", señala Vázquez. Esta consulta sistemática reveló la demanda de cursos especializados en ciberseguridad que pudieran marcar una diferencia significativa para los profesionales de la región.

Construyendo el caso de éxito

La decisión de colaborar con SANS Institute para impartir la formación en ciberseguridad respondió a una clara motivación estratégica. «*A la hora de determinar la necesidad de la formación de SANS, se tuvo en cuenta que su formación es prestigiosa y reconocida por todo el mercado, tanto por los profesionales de la ciberseguridad como por las empresas del sector*», explica Vázquez. Un factor clave de la formación de SANS es que los cursos ofrecen la oportunidad de obtener certificaciones GIAC. Estas credenciales, reconocidas por la industria, validan competencias específicas en materia de ciberseguridad. Este componente de certificación resultaría crucial para el éxito del programa.

El argumento comercial para invertir en formación de ciberseguridad de alta calidad no fue fácil de plantear. «*Es una formación de calidad, pero significativamente más cara que otras*», reconoce Vázquez. Sin embargo, su argumento ante los líderes regionales se centró en la ventaja competitiva a largo plazo: «*Los profesionales que completan esta formación obtienen una ventaja competitiva que hace que la inversión merezca la pena. Aunque los cursos pueden ser más costosos que otras alternativas, dotan a nuestros profesionales de cualificaciones especializadas y certificaciones que abren puertas en el mercado laboral nacional e internacional*».

[1] https://cds.thalesgroup.com/en/hot-topics/spain-fifth-country-most-ransomware-threats-2024

Midiendo el éxito del programa

El programa de ciberseguridad del CNTG está abierto a todos los ciudadanos de Galicia, estén empleados o desempleados. Sin embargo, como explica Vázquez, los participantes son principalmente "*profesionales del sector TI gallego que se dedican a la ciberseguridad*".

La respuesta de los participantes ha sido abrumadoramente positiva. "*Al final de cada curso, hacemos una evaluación. Los estudiantes valoran la calidad de esa formación, y esta evaluación ha sido muy positiva, con puntuaciones superiores a 9 sobre 10*", informa Vázquez. El feedback cualitativo es igualmente revelador: "*El comentario que escuchamos de los participantes es que tener acceso a esta formación en Galicia es un lujo*".

> *«La certificación es un elemento clave para los profesionales, ya que las empresas reconocen que quienes la obtienen cuentan con competencias avanzadas en ciberseguridad.»*

El CNTG mide el éxito a través de tres métricas clave: niveles de demanda, satisfacción inmediata de los participantes y evaluaciones del impacto profesional a los seis meses. Los resultados validan la inversión, y el componente de certificación GIAC ofrece retornos particularmente sólidos.

El reconocimiento que el mercado otorga a las certificaciones GIAC ha generado un círculo virtuoso. Tanto los profesionales como los empleadores comprenden su valor, lo que impulsa una demanda sostenida.

«*La certificación es un elemento clave para los profesionales, ya que las empresas reconocen que quienes la obtienen cuentan con competencias avanzadas en ciberseguridad». Algunas personas han mejorado profesionalmente dentro de su propia organización o han accedido a nuevas oportunidades laborales en otras empresas, logrando un avance en su carrera profesional*», explica Vázquez.

Más allá del desarrollo profesional individual, las personas que cuentan con certificaciones GIAC han permitido a sus empresas acceder a licitaciones o proyectos que anteriormente no estaban a su alcance. Las certificaciones actúan como una prueba tangible de competencias y han abierto nuevas oportunidades de negocio. Como señala Vázquez, las certificaciones se han convertido en un elemento esencial en los procesos competitivos: «*En muchas licitaciones se exigen certificaciones específicas para el proyecto. Si no se puede acreditar que los miembros del equipo disponen de dichas certificaciones, se queda automáticamente excluido*».

Implicaciones estratégicas más amplias

El éxito del programa ha llevado a una expansión significativa. Comenzando en 2024 con 20 estudiantes anuales que recibían formación en **SEC504 (Hacker Tools, Techniques, and Incident Handling)** y **FOR508 (Advanced Incident Response, Threat Hunting, and Digital Forensics)**, el CNTG está evaluando añadir las formaciones **SEC556 (Internet-of-Things Penetration Testing)** y **FOR572 (Advanced Network Forensics)** al plan de estudios. "*La expansión refleja el compromiso del gobierno gallego con la formación en ciberseguridad*", señala Vázquez. "*Lanzaron un nuevo proyecto y decidieron incluir cursos adicionales de SANS y certificaciones GIAC porque han visto lo valiosos que son para los profesionales gallegos*".

El proceso de selección de cursos reproduce el enfoque original, que implica una extensa consulta con actores de la ciberseguridad de toda la región. "*Amtega habla con todos los agentes públicos y privados para decidir cuáles son los cursos que marcan la diferencia para los profesionales*", señala. Este enfoque colaborativo garantiza que la formación se mantenga alineada con las necesidades reales del mercado.

Las comunidades autónomas de España operan de forma independiente en términos de asignación presupuestaria y decisiones de política, lo que hace que el enfoque de Galicia sea particularmente significativo como modelo potencial para otras regiones. El gobierno español ha anunciado una inversión de 1.100 millones de euros[2] para mejorar la ciberseguridad, con un enfoque en proteger infraestructuras críticas y mejorar la resiliencia. Además, se han destinado miles de millones de euros a capacidades de telecomunicaciones y ciberseguridad a través de diversos planes nacionales.

> *«Todo se reduce al retorno de la inversión: la formación de SANS es exigente en coste, pero genera un retorno sobresaliente al elevar el nivel de cualificación de los profesionales.»*

El programa del CNTG demuestra cómo los gobiernos regionales pueden contribuir de manera significativa a los objetivos nacionales de ciberseguridad mientras construyen ventaja competitiva local. "*Para nosotros, la ciberseguridad es un elemento importante en la formación en TI. De hecho, en este momento es el elemento más importante en la formación del centro*", enfatiza Vázquez. SANS se ha convertido en parte integral de esta estrategia: "*Es un excelente proveedor de formación en ciberseguridad*".

Para otros gobiernos regionales que consideren inversiones similares, Vázquez ofrece un consejo pragmático: «*Todo se reduce al retorno de la inversión: la formación de SANS es exigente en coste, pero genera un retorno sobresaliente al elevar el nivel de cualificación de los profesionales*». Lo enmarca como una necesidad estratégica: "*Simplemente diría que esta es una formación en la que otras entidades deberían invertir porque establece un elemento diferencial para sus ciudadanos o profesionales. Para nosotros, es una apuesta segura, una inversión segura*".

[2] https://digital.gob.es/en/comunicacion/notas-prensa/mtdfp/2025/05/2025-05-06_02

Inversiones estratégicas

El enfoque de Galicia hacia la formación pública en ciberseguridad ofrece un modelo de cómo los gobiernos regionales pueden construir resiliencia cibernética a través del desarrollo estratégico del talento. Las métricas de éxito hablan por sí mismas: alta satisfacción de los participantes, avance profesional medible, mayor competitividad regional y una demanda creciente que llevará a expandir el programa. Más importante aún, el programa ha creado un modelo sostenible donde la inversión pública en formación en ciberseguridad genera retornos en toda la economía regional.

Para los líderes en ciberseguridad que consideren asociaciones público-privadas similares, la experiencia de Galicia demuestra que las inversiones estratégicas en el desarrollo del talento pueden abordar simultáneamente las carencias inmediatas de competencias mientras se construye resiliencia cibernética regional a largo plazo. En un mundo cada vez más conectado donde las ciberamenazas no conocen fronteras, estos enfoques colaborativos bien pueden representar el futuro de una defensa cibernética eficaz.

SANS Training at CNTG

SEC504: Hacker Tools, Techniques, and Incident Handling) | GCIH

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics | GCFA

SEC556: IoT Penetration Testing

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GNFA

SANS Institute

The most trusted source for cybersecurity training, certifications, degrees and research.

Contact Us

+44 203 384 3470

www.sans.org

emea@sans.org

@sansemea

CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA

SANS